

## 1/29/08 Legendre's Theorem

A conic is an absolutely irreducible curve of degree 2. Given by  $f(x, y) = 0$  where  $\deg f = 2$ .

If we are looking for rational solutions of an equation  $f(x, y) = 0$  where  $\deg f = d$ , we can also look at the homogenous polynomial of degree  $d$  in  $x, y, z$  given by  $z^d f(x/z, y/z)$ . We have to be careful with  $z = 0$ .

A conic can be further simplified by diagonalization. So we can reduce the study of conics to equations of the form  $ax^2 + by^2 + cz^2 = 0$  where absolute irreducibility is equivalent to  $abc \neq 0$ .

If  $a, b, c \in \mathbb{Q}$  and we want to find out if  $ax^2 + by^2 + cz^2 = 0$  has solutions, we can assume that  $a, b, c \in \mathbb{Z}$  by clearing denominators. We can also assume that  $a, b, c$  have no common factors.

If  $a = m^2 \cdot a'$  then  $ax^2 + by^2 + cz^2 = 0$  has a solution if and only if  $a'x^2 + by^2 + cz^2 = 0$  has a solution (replace  $x$  by  $mx$ ). In this way we can assume that  $a, b, c$  are square free.

Suppose there exists a prime  $p$  such that  $p$  divides both  $a$  and  $b$ . Then  $a = a' \cdot p$  and  $b = b' \cdot p$ . If  $ax^2 + by^2 + cz^2 = 0$  has a solution then

$$pa'x^2 + pb'y^2 + cz^2 = 0$$

$$a'(px)^2 + b'(py)^2 + pcz^2 = 0$$

has a solution. Proceeding in this way, I can eliminate common factors of any two of  $a, b, c$ .

**Legendre's Theorem.** *Suppose that  $a, b, c \in \mathbb{Z}$  are nonzero, square free, and pairwise coprime. Then the equation  $ax^2 + by^2 + cz^2 = 0$  has a solution in  $\mathbb{Z}^3 - \{(0, 0, 0)\}$  if and only if the following two conditions are satisfied.*

- (i)  $a, b, c$  are not all of the same sign.
- (ii) For all odd primes  $p \mid abc$  there is a solution to  $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$  where all of  $x, y, z \not\equiv 0 \pmod{p}$

**Proof.** ( $\uparrow$ ) If  $p \mid abc$  assume that  $p \mid a$ . We are assuming that  $\exists x_0, y_0, z_0 \not\equiv 0 \pmod{p}$  with  $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{p}$  which is equivalent to  $by_0^2 + cz_0^2 \equiv 0 \pmod{p}$ . Let

$$u^2 = -\frac{b}{c} = \left(\frac{z_0}{y_0}\right)^2$$

As a polynomial,

$$\begin{aligned}
ax^2 + by^2 + cz^2 &\equiv by^2 + cz^2 \pmod{p} \\
&\equiv c(z^2 - u^2y^2) \pmod{p} \\
&\equiv c(z - uy)(z + uy) \pmod{p}
\end{aligned}$$

So for every odd prime  $p \mid abc$  there are linear forms  $L_p$  and  $L'_p$  in  $x, y, z$  with

$$ax^2 + by^2 + cz^2 \equiv L_p L'_p \pmod{p}$$

Also, for  $p = 2$ ,

$$ax^2 + by^2 + cz^2 \equiv (ax + by + cz)^2 \pmod{2}$$

So there is also  $L_2$  and  $L'_2$  such that

$$ax^2 + by^2 + cz^2 \equiv L_2 L'_2 \pmod{2}$$

By the Chinese Remainder Theorem, there exist linear forms  $L$  and  $L'$  such that

$$ax^2 + by^2 + cz^2 \equiv LL' \pmod{abc}$$

Consider integers  $x_0, y_0, z_0$  that satisfy the inequalities

$$0 \leq x_0 \leq \sqrt{|bc|}$$

$$0 \leq y_0 \leq \sqrt{|ac|}$$

$$0 \leq z_0 \leq \sqrt{|ab|}$$

Since  $a, b, c$  are square free and coprime, we actually have

$$0 \leq x_0 < \sqrt{|bc|}$$

$$0 \leq y_0 < \sqrt{|ac|}$$

$$0 \leq z_0 < \sqrt{|ab|}$$

How many such triples are there? The answer is greater than

$$\left(1 + \lfloor \sqrt{|bc|} \rfloor\right) \left(1 + \lfloor \sqrt{|ac|} \rfloor\right) \left(1 + \lfloor \sqrt{|ab|} \rfloor\right) > |abc|$$

By the Pigeon Hole Principle there exists distinct such triples  $(x_0, y_0, z_0)$  and  $(x'_0, y'_0, z'_0)$  with

$$L(x_0, y_0, z_0) \equiv L(x'_0, y'_0, z'_0) \pmod{abc}$$

which implies that

$$L(x_0 - x'_0, y_0 - y'_0, z_0 - z'_0) \equiv 0 \pmod{abc}$$

and consequently

$$a(x_0 - x'_0)^2 + b(y_0 - y'_0)^2 + c(z_0 - z'_0)^2 \equiv 0 \pmod{abc}$$

Let  $x = x_0 - x'_0$ ,  $y = y_0 - y'_0$  and  $z = z_0 - z'_0$ . Then

$$|x| < \sqrt{|bc|}$$

$$|y| < \sqrt{|ac|}$$

$$|z| < \sqrt{|ab|}$$

and

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{abc}$$

By condition (i) we may suppose without a loss of generality that  $a < 0$ ,  $b < 0$ , and  $c > 0$ . This implies that  $|abc| = abc$ . As a result

$$ax^2 + by^2 + cz^2 \leq cz^2 < abc$$

$$-(|a|x^2 + |b|y^2) \leq ax^2 + by^2 + cz^2$$

$$-2abc < -( |a|x^2 + |b|y^2 )$$

so that

$$-2abc < ax^2 + by^2 + cz^2 < abc$$

and

$$ax^2 + by^2 + cz^2 = 0 \text{ or } -abc$$

If  $ax^2 + by^2 + cz^2 = 0$ , then we are done. We thus suppose that

$$ax^2 + by^2 + cz^2 = -abc$$

$$ax^2 + by^2 + c(z^2 + ab) = 0$$

Since  $a$  and  $b$  are squarefree and coprime,  $z^2 + ab \neq 0$ . The proof of the  $\uparrow$  direction is complete by the following polynomial identity.

$$a(xz + by)^2 + b(yz - ax)^2 + c(z^2 + ab)^2 = (ax^2 + by^2 + c(z^2 + ab))(z^2 + ab) = 0$$

**Proof.** ( $\Downarrow$ ) Suppose that  $ax^2 + by^2 + cz^2 = 0$  where  $x, y, z \in \mathbb{Z}$  are not all zero. Let  $p$  be an odd prime. If  $p$  divides  $x, y$  and  $z$  then

$$a\left(\frac{x}{p}\right)^2 + b\left(\frac{y}{p}\right)^2 + \left(\frac{z}{p}\right)^2 = 0$$

We may thus suppose that  $p$  does not divide one of  $x, y$ , or  $z$ . If  $p$  divides  $x$  and  $y$  but not  $z$  then it follows that  $p^2$  divides  $cz^2$  and therefore that  $p^2$  divides  $c$ .  $c$  was assumed to be square free. This is a contradiction. So  $p$  can divide at most one of  $x, y$ , and  $z$ .

Suppose that  $p$  divides  $a$  and  $x$  but not  $y$  or  $z$ . From  $ax^2 + by^2 + cz^2 = 0$  we have

$$a1^2 + by^2 + cz^2 \equiv 0 \pmod{p}$$

Suppose that  $p$  divides  $a$  and  $y$  but not  $x$  or  $z$ . Then

$$0 = ax^2 + by^2 + cz^2 \equiv cz^2 \pmod{p}$$

So  $p$  divides  $c$ . This is a contradiction since  $a$  and  $c$  are coprime.  $\square$

### **New Topic: P-Adic Numbers**

Let  $p$  be a prime number. For  $x \in \mathbb{Q}$ ,  $x \neq 0$  we can write

$$x = p^r \cdot \left(\frac{a}{b}\right)$$

with  $a, b, r \in \mathbb{Z}$  and  $p \nmid ab$ .

The  $p$ -adic norm of  $x$  is defined as  $|x|_p = p^{-r}$  and  $|0|_p = 0$ .  
The  $p$ -adic distance from  $x$  to  $y$  is defined as  $d_p(x, y) = |x - y|_p$ .

**Exercise:** Prove that  $d_p$  is a metric.

$\mathbb{Q}_p$  is the completion of  $\mathbb{Q}$  with respect to the metric  $d_p$ .

$\mathbb{Z}_p$  is the completion of  $\mathbb{Z}$  with respect to the metric  $d_p$ .

**Exercise:** Show that  $\mathbb{Q}_p$  is a field,  $\mathbb{Q} \subseteq \mathbb{Q}_p$  and  $\mathbb{Z}_p$  is a ring,  $\mathbb{Z} \subseteq \mathbb{Z}_p$ .

Every element of  $\mathbb{Q}_p$  is of the form

$$x = \sum_{n=n_0}^{\infty} a_n p^n$$

where  $a_n \in \{1, \dots, p-1\}$ ,  $a_{n_0} \neq 0$  and  $|x|_p = p^{-n_0}$ .

We note the **ultrametric inequality**. For  $x, y \in \mathbb{Q}_p$ ,

$$|x + y|_p \leq \max\{|x|_p, |y|_p\}$$

$\mathbb{Z}_p$  is a local ring with maximal ideal  $(p)$ .

$\frac{1}{1-p} = \sum_{n=0}^{\infty} p^n \in \mathbb{Z}_p$ . So  $1-p$  is a unit.

**Exercise:** Show that for all  $a \in \mathbb{Z}$ ,  $p \mid a$ ,  $a$  is a unit in  $\mathbb{Z}_p$ .

$$\frac{\mathbb{Z}_p}{(p^n)} \cong \frac{\mathbb{Z}}{p^n \mathbb{Z}}$$

**Exercise:** Show that  $\mathbb{Z}_p$  is isomorphic to

$$\begin{aligned} \lim_{\leftarrow} \frac{\mathbb{Z}}{p^n \mathbb{Z}} &:= \{(a_1, a_2, \dots) \mid a_i \in \frac{\mathbb{Z}}{p^i \mathbb{Z}}, a_{i+1} \equiv a_i \pmod{p^i}\} \\ &\subseteq \frac{\mathbb{Z}}{p \mathbb{Z}} \times \frac{\mathbb{Z}}{p^2 \mathbb{Z}} \times \dots \end{aligned}$$

**Theorem.** The following are equivalent.

(i)  $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$  such that  $\forall r \exists$  solutions to  $f(x_1, \dots, x_n) \equiv 0 \pmod{p^r}$ ,  $x_i \in \mathbb{Z}$ .

(ii)  $\exists$  solutions to  $f(x_1, \dots, x_n) = 0$  with  $x_i \in \mathbb{Z}_p$ .

**Proof.** (i)  $\implies$  (ii)

For each  $r$  let  $x_1^{(r)}, \dots, x_n^{(r)} \in \mathbb{Z}$  with  $f(x_1^{(r)}, \dots, x_n^{(r)}) \equiv 0 \pmod{p^r}$ . Since  $\mathbb{Z}_p$  is compact  $\exists$  a convergent subsequence for the  $x_i^{(r)}$  and the limit satisfies  $f(x_1, \dots, x_n) = 0$